Emerging drone trends for blockchain-based 5G networks: open issues and future perspectives

Article (Accepted Version)

Emerging Drone Trends for Blockchain-Based 5G Networks: Open Issues and Future Perspectives

Tao Han[1,*], Igor de L. Ribeiro[2], Naercio Magaia[3], João Preto[3], Afonso H. Fontes N. Segundo[2], Antônio Roberto L. de Macêdo[2], Khan Muhammad[4,*], and Victor Hugo C. de Albuquerque[2]

[1] DGUT-CNAM Institute Dongguan University of Technology, Dongguan, China
[2]University of Fortaleza, Fortaleza - CE, Brazil
[3]LASIGE, Department of Computer Science, Faculty of Sciences, University of Lisbon, Portugal
[4]Department of Software, Sejong University, Seoul, Republic of Korea
[*]Corresponding Authors: Khan Muhammad (khan.muhammad@ieee.org) and Tao Han (hant@dgut.edu.cn)

Abstract

Unmanned Aerial Vehicles (UAVs), also commonly known as drones, are receiving growing research interest due to their ability to carry a multitude of sensors and to connect to mobile networks. They are also able to move freely across the air, which enable the creation of numerous applications that were up until now considered impracticable. However, such applications may require high computational resources, reliable connection, and high data transmission rates to accomplish different tasks. Therefore, in this work, first, we discuss 5G communication networks and Mobile Edge Computing (MEC) as promising technologies that can provide several benefits to drone-enabled environments and solve some of the presented issues. We also comment on 5G and MEC approaches, presenting state-of-the-art and seeking at solving each of the latter issues presented. Afterward, we introduce new security concerns of drone communication networks, given their recent popularity. These concerns are related to the possibility of malicious users taking advantage of this brand-new technology, which made many governments ban drones due to public safety. Next, Blockchain technology is brought as a novel solution to the security issues, which raised its decentralized nature, making it inherently safe. This article also surveys contributions that make use of each of the technologies mentioned to improve the emerging drone industry. Subsequently, we discuss open issues and future perspectives.

Keywords

Drones, 5G, Communication Networks, Blockchain, Edge Computing.

1 Introduction

The increase in popularity and affordability of Unmanned Aerial Vehicles (UAVs), also commonly known as drones, has resulted in growing attention from researchers and businesses in developing novel technologies, algorithms, and applications. The latter happened in many different fields because of drones' ease of use, high-mobility, and ability to hover. Researchers already view drones as valuable service providers for future smart cities performing various roles, such as delivering goods and merchandise, maintaining surveillance, traffic monitoring, as well as increasing wireless network coverage [1], [2]. However with the emerging Internet of Things (IoT) framework and the related enabling technologies, such as the Device-to-Device (D2D) paradigm, the fifth-generation mobile technology (5G standard), and cloud/fog computing come with significant security, privacy, and public safety concerns that need to be discussed [3].

The Blockchain technology comes as a promising solution to the data privacy concerns that surround the drone-related frameworks discussed above. A blockchain is a secured, shared, and

distributed ledger that facilitates the process of recording and tracking resources without the need for a centralized trusted authority [4], [5].

This article focuses on studying the interaction of drones with wireless networks that can support their personal or professional use and current challenges posed by integrating novel drone technology into cellular networks for better control and communication. For example, current challenges include balancing drone weight, battery capacity, and computational resources. Many other existing surveys have proposed studying the applicability of flying ad hoc networks in 5G-enabled environments. For instance, Zhang et al. [6] present a taxonomy for classifying the latest achievements of 5G millimeter wave (mmWave) communications in UAV-assisted networks. They also provide vital technological benefits and challenges besides desirable applications for this newly emerging area. Salman et al. [4] present a survey on the recent achievements made in blockchain-based security services and applications to provide more secure networks for User Equipment (UE). Such services include authentication, confidentiality, privacy, and access control list, data and resource provenance, and integrity assurance, which are crucial for the current distributed applications. Fotouhi et al. [7] present a survey on UAV cellular communication, introducing the types of consumer UAVs currently available and standardization advancements made to smoothen the integration of UAVs into cellular networks. However, in this article, we provide an original survey on blockchain-based technologies used in the assistance of UAV-enabled networks to provide better Quality of Service (QoS) and Quality of Experience (QoE) for users. The key contributions can be summarized as follows:

- We introduce a novel 5G communication network and its applicability within a drone framework. We present main challenges such as reliability and connectivity issues and highlight novel research contributions that can solve those issues.
- We propose a new paradigm for the future of mobile networks involving drones, 5G, edge computing, IoT technologies, and how their integration can benefit the network and improve QoS.

The rest of the paper is organized as follows: Section 2 gives a brief background on 5G-enabled networks and discusses the research contributions based on reliability, connectivity, and energy efficiency. Section 3 introduces Blockchain, its advantages, and disadvantages for UAV-assisted networks. Section 4 discusses the relationship between MEC, IoT, and 5G in UAV-based networks. Section 5 presents open issues and future research directions. Finally, Section 6 presents concluding remarks of this study.

2 5G Communication Network

The fifth-generation mobile communications system (5G) is the new generation of wireless technology for cellular networks. In this technology, one of the potential solutions proposed to ensure a high transmission rate is to enlarge higher frequencies' usage in the radio spectrum [8]. The reason is that a large number of usable spectrum bands remain untouched and are feasible to be explored at these frequencies. As such, researchers have recognized the benefits of utilizing mmWave frequencies ranging from 30 GHz to 300 GHz as a promising method for achieving multiple Gigabit data transmission speeds [6].

The need for a communication network that could support the demand for a higher data rate sufficiently fostered the increased interest in the development of drone technology. 5G has been seen as a possible solution to address the demand for better transmission rates in mobile networks.

The development of mobile networks and drone research are closely related as most drone applications make use of mobile networks to provide direct or indirect connectivity to other UE [6]. Vehicular Networks (VNs) are another research area, where drones are receiving spotlight as

valuable contributors to MEC-enabled architectures. That is due to their ability to provide computational resources to networks and improve coverage signal and quality to Road Side Units (RSUs) during heavy traffic. However, the integration of drones in vehicular networks presents several challenges that require more research. Shi et al. [2] highlight the main challenges that have emerged in this direction:

(i) Mobility control schemes for drones: Organizing the drones' mobility taking into consideration collision avoidance, flying route definition, drone swarm formations, among others. Designing an adaptable network of exchangeable information between vehicles;

(ii) Internetworking between drones and ground networks: Forming network mechanisms that allow communication between flying nodes, ground nodes, and infrastructure is vital for accomplishing ubiquitous connections.

(iii) Efficient power consumption of drones: Ensuring the highest operational time possible is a constant struggle for drone applications, as they have to balance power between communication and flying control.

(iv) Regulation and security issues in drone assisted vehicular network (DAVN): The exploitation of drones' vulnerabilities by malicious users may jeopardize both the device and network hence threatening public safety.

Figure 1 shows a UAV-assisted network where a drone works as an Aerial Base Station (ABS) to provide better signal coverage and enables other applications. The vehicle-to-vehicle (V2V) link between V1 and UAV1 is an example of a communication link between drones and vehicles where the 5G network is assisting the MEC-enabled vehicular environment. UAV1, UAV2, and UAV3 are utilizing Aerial-to-Ground (A2G) 5G mmWave beams to enhance wireless coverage and provide high transmission speeds towards physical objects including ground UEs in vehicle-to-person (V2P), V2V, and vehicle-to-infrastructure (V2I) communications.

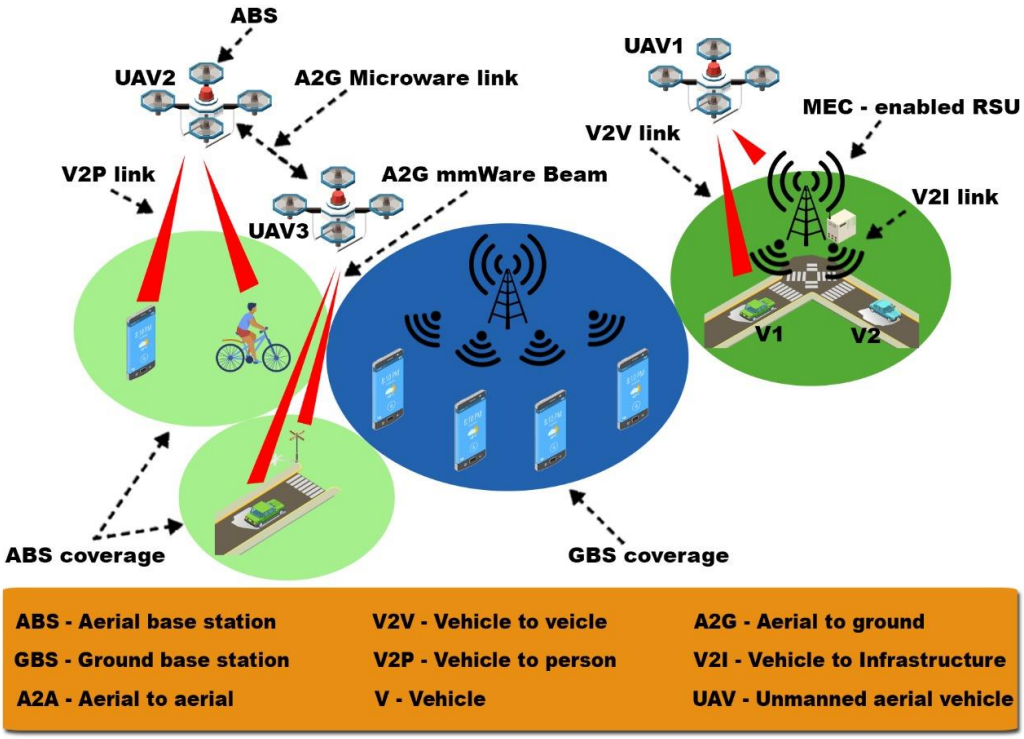

Figure 1. An overview of the 5G-enabled drone architecture in the field and representation of the drone-assisted Base Station application.

2.1 Reliability

The dynamic nature of drone-based environments makes it difficult to maintain a reliable and stable connection to ensure satisfactory QoS and QoE for UEs. QoS and QoE directly impact one another, therefore, it is essential to manage each factor based on which aspect of their service is more affected and make adjustments accordingly. For example, one of the emerging technologies in the drone industry is the use of drones as monitoring devices that can map a particular area and alert for either anomalies or intruders [3]. In the latter application, it is far more critical to ensure that the drone will not file alerts for trivial objects entering the monitored area, such as leaves or small birds. As such, the reliability of the information is of vital importance.

Many researchers have investigated technologies to enhance network reliability. For instance, R. Guimaraes et al. [9] used an optimum-path forest-based approach for modeling a problem of failure identification in Wireless Sensor Networks, aiming to increase the reliability of anomaly detection task related applications. Meanwhile, not directly tailored towards drone use, the proposed approach can efficiently be utilized for safety or monitoring drone services. On the other hand, V. Sharma et al. [10] proposed a neural-blockchain based ultra-reliable caching for drone-supported networks focusing primarily on improving latency and reliability in the Mobile Edge Computing (MEC) infrastructure. They treat vehicles (i.e., drones) as edge computation resources and constructs a blockchain model between them to maintain a reliable connection in a 5G core network. 5G core architecture is designed to exploit better the advantages of Network Function Virtualization (NFV) and Software-Defined Networking (SDN), enable automation and improve flexibility, allowing a Network Function (NF) to talk to other NFs directly [8].

2.2 Availability / Connectivity

Similar to the reliability challenges presented, stable connectivity is vital for drone-based technology to meet satisfactory QoS and QoE. Here, connectivity is defined as the network's ability to ensure resource availability to complete a specific task and consistently maintaining a stable connection between all networks of the UE, drones, and Base Stations (BSs). Losing connection may be considered as the worst-case scenario for some applications. Therefore, some technologies have emerged that could assist the network through the use of drones as BSs with 5G communication technology to provide seamless service and high data rates to UEs [8].

Shi et al. [11] proposed a 3D trajectory planning of multiple drone BSs in which the optimization of drone BS takes into account both the flying heights and horizontal trajectories, aiming at minimizing the average device-to-user (D2U) path loss. In this context, the authors envisioned a static drone BS deployment as a means to improve the user's QoS and network performance by strategically deploying the drone in areas to provide wide-area connectivity and enhanced signal coverage. Moreover, Del et al. [12] proposed architecture for 5G wireless networks where they integrate Artificial Intelligence (AI) and Blockchain technology into wireless networks enabling flexible and secure resource sharing intending to maximize resource utilization through Deep Reinforcement Learning (DRL).

2.3 Energy Efficiency

One of the recurring challenges regarding drone research is the constant concern of running out of battery or making a service/algorithm that can make use of the potential computational resources of drones while simultaneously conserving the drone's battery life. A worst-case scenario for drone services is to have an application spending unreasonable resources to fulfill a task and draining the battery life, which would cause the drone to go into battery saving mode and land, ceasing its network functionalities. It would also cause possible coverage signal holes or potentially losing cargo in "pick-up and drop-off" drone services.

Balancing drone weight, battery capacity, and computational resources is another constant adversity faced by drone services developers, and numerous researchers have taken different approaches to tackle this issue. For instance, Yang et al. [13] proposed a DRL method to develop an efficient movement control algorithm for multiple drone-cells in a three-dimensional continuous movement environment to maximize the energy-efficiency of communication coverage of drone-cell networks while preserving the network connectivity.

Table 1 summarizes the contributions made by the research community in enhancing reliability, connectivity, and energy efficiency in systems. In addition, the main algorithm is highlighted, and the advantages/disadvantages are discussed.

Table 1. Reliability, connectivity/availability, and energy-efficient approaches

Issue	**#**	**Solution (or proposed solution)**	**Advantages**	**Disadvantages**
Reliability	[10]	Neural-blockchain based algorithm	-Decreases energy consumption - Reliability remains high for a dense user population	Possibility of path loss in alternative routes
	[9]	Optimum-path based approach for anomaly detection tasks	Most accurate technique under The Intel Berkeley Research Laboratory (IBRL) and Grand St. Bernard (GSB) datasets	The results show that other techniques can also achieve similar performance
Availability	[11]	3D trajectory planning and scheduling algorithm	Reduces path loss from data to the user	Does not propose how to allocate resources between the multiple drone base stations
	[12]	Deep Reinforcement Learning-based algorithm.	Improves resource allocation in 5G wireless networks	Does not show the computational load required in the proposed scheme
Energy Efficiency	[13]	DRL algorithm.	Considers QoS requirements while maintaining high energy efficiency	Does not consider interference among adjacent drone-cells.

3 Blockchain, Advantages, and Challenges regarding Communication

Blockchain consists of a ledger of transactions which are assembled into blocks created by miners who are required to supply a Proof-of-Work (PoW). While different types of proofs have been proposed, such as Proof-of-Retrievability (PoR), PoW remains the standard in most Blockchain implementations. These blocks contain a hash of the previews block in such a way as to create a "chain". Nodes then keep track of blocks as they are broadcast to the network, checking the correctness of the PoW and the validity of the transactions it contains. If two blocks are mined simultaneously, this creates a fork. To solve this problem, the longest chain is regarded as the correct one, as this is the one that has had more work put into it. The latter also ensures that any attack must control more than half of the mining power to succeed.

3.1 Advantages and Disadvantages

The main contribution of the Blockchain technology is the possibility to benefit from security assurances that are usually provided by a centralized trusted authority (wherein the case of bitcoin this authority would be a bank or an electronic alternative such as PayPal). Jensen et al. [1] provide a good example of areas where UAV systems can benefit from Blockchain implementations, namely:

(i) Confidentiality: The use of a private or consortium based Blockchain to limit who can see data in the system, and place restrictions on who can participate in it, also known as permissioned blockchains. The utilization of Public Key Infrastructure (PKI), i.e., a tool that is already used by Blockchain mainly to assign ownership of resources, to encrypt data blocks within the Blockchain, and provides more confidentiality.

(ii) Integrity: Due to the underlying mechanisms of Blockchain, any forks that may be created will inevitably be abandoned as miners shift focus to the largest chain of blocks available. Because of this, one of the main characteristics of Blockchain is immutability. This characteristic helps ensure high data coherence because once information is added to the ledger, users can trust that the transactions on the ledger are credible [1]. Besides, they argue that the use of digital signatures enables Blockchain to be fully traceable, providing transparency as well as security. Furthermore, the development of smart contract technologies allows parties to establish and ensure rules between one another, further increasing the system's data integrity.

(iii) Availability: Decentralization improves availability by removing a single point of failure. In the case of attack, and if the attacker targets specific nodes, they can be excluded from the network. Therefore, it is possible to continue operating with all the other nodes.

UAVs need to be as light as possible to facilitate its flying operations. Consequently, they are resource-constrained devices (i.e., limited computational power, storage, etc.). However, most Blockchain implementations use highly computational demanding PoW. Other approaches, such as PoR, are similarly impractical as they require a high amount of disk space. The constrained disk storage also poses a difficulty as full nodes require a local copy of the entire Blockchain, which occupies about 240GB in the case of bitcoin and 180GB in the case of Ethereum [4].

Recent Blockchain applications such as Ethereum, provide what is called smart contracts, that is, small pieces of runnable code that can be performed when a transaction is made to a specific address. While a UAV might not have the possibility to participate in a Blockchain as a miner due to their lack of substantial computational power, they could offload the hard work of transaction verification to more powerful nodes of the network, hence enjoying many of the security benefits this technology provides. Another approach is to utilize permissioned blockchains as they allow for the utilization of easy to solve consensus algorithms [1], [11], [14]. In addition, light nodes have been proposed to enable storage to limited devices to participate in Blockchain networks.

3.2 Solutions

V. Sharma et al. [10] proposed the utilization of neural networks and a combination of three Blockchain ledgers to accomplish drone-caching for ultra-reliable networks utilizing MEC. The proposed approach performs well regarding metrics such as connectivity, survivability, and reliability. Jensen et al. [1] utilized Hyperledger Fabric to create a private permissioned blockchain that enables the creation and maintenance of a UAV swarm network. They accomplish this by defining certain drones as Master ones that control Slave drones through transactions in the ledger. Nevertheless, it is also considered very feasible the development of custom solutions leveraging Blockchain, if, for UAVs, there are achieved compromises between computational and

energy limitations. Lei et al. [14] demonstrate that poisoned content can present a severe problem in named-data networking (NDN) used in unmanned aerial vehicle ad hoc networks (UAANETs). To solve this problem, they utilize a permissioned blockchain to maintain a decentralized record of interest-key-content binding rules. Dai et al. [11] proposed a state-of-the-art framework for next-generation wireless networks that makes heavy use of AI and Blockchain technologies, ensuring a secure and private communication environment. They provide a few examples where Blockchain would be beneficial, namely spectrum sharing, D2D caching, energy trading, and computation offloading.

4 5G, Drones and Edge Computing

MEC is a promising area of study among next-generation vehicular networks (i.e., Internet of Vehicles – IoV) researchers, which was enabled by the development of 5G mobile networks. MEC is a widely distributed network architecture that treats each device at the edge of the network as nodes with computation capabilities. It allows UE to offload data directly to nearby servers providing multiple benefits such as high bandwidth, computational agility, and low latency.

The inherent capabilities of drones can assist in enhancing network performance in various ways, as they are mobile devices that can freely navigate in open areas and connect to cellular networks while also potentially being capable of performing some computational tasks. This opens up the opportunity to connect with various types of infrastructures when merging VN, IoT, and 5G through V2V, V2I, and vehicle-to-device (V2D) that makes various features possible. Shi et al. [2] highlight some of these features as follows:

(i) Line-of-sight (LoS) links: Through LoS links, drones can utilize real-time traffic information collected by its sensors to adjust their position within the network to maintain reliable connectivity, hence adjusting to the network's needs.

(ii) Dynamic deployment ability: Unlike the traditional structure, drones can fly and maneuver over the desired space, which allows them to change their position dynamically based on the user's demand;

(iii) Drone swarm networks: Apart from infrastructures, a swarm of drones is capable of forming scalable drone swarm networks allowing ground nodes to access.

(iv) Providing connectivity for resource-less scenarios: Drones can be used as Aerial Base Stations (ABS) to provide better connectivity for coverage holes, when the current infrastructure cannot support the network demand from users, therefore acting as a temporary assisting service for networks.

However, the features mentioned above are only feasible in a 5G-assisted communication network due to their reliance on high transmission rate and low latency. The need to accommodate diverse types of users, applications with diverse performance requirements, and the need to integrate heterogeneous air interfaces into the next-generation wireless networks are likely to make the radio spectrum more congested [11]. 5G mmWave communication comes as a promising technology given their extremely wide bandwidths, small element sizes, and narrow beams that is beneficial if compared to existing wireless technologies [15]. Furthermore, narrow beams are particularly interesting for drone usage as they can pack more frequencies in a narrower beam, which can facilitate the development of applications such as detection radars.

5 Open Issues and Future Perspectives

Modern drones can be equipped with various sensors, wireless communication, and computational capabilities that enable the use of various services to improve QoE for users. The development of IoT research has brought immense value to drone networks, and the integration of technologies such as 5G, MEC, and drones has led to a growing interest in IoV research. However, numerous challenges have yet to be resolved regarding drone-based technologies, such as:

- Balancing drone weight, battery capacity, and computational resources remains the biggest obstacle for developing new drone-based technologies.
- As a result of the unique nature of the technologies discussed, the lack of a simulation model makes it difficult to compare approaches effectively.

Although most researchers understand the need to be energy efficient, many research studies do not take battery life, device weight, and computational limitations when evaluating their performance, diminishing their real-life applicability. Nonetheless, recent studies regarding drone battery life focus on achieving better energy efficiency through the use of algorithms to guarantee high movement efficiency and resource utility. However, battery life is still a prevalent issue. Hence, new approaches to solve the latter are advocated that take a different path through energy efficiency driven algorithms.

6 Conclusion

This article has introduced a couple of technologies that have been used to enhance drone-based services, explicitly MEC, 5G, and Blockchain. Each of these technologies is shown to bring several benefits to drone technologies, and increase, in general, the QoS and QoE of the users. Although these approaches bring many benefits, there are still a few challenges that need to be addressed in order to increase the real-life applicability of such applications to maximize connection reliability, network availability, energy efficiency, and security.

IoT, VNs, and drones are trending topics that get influenced by new technologies in several fields, as with the latter, the applicability of diverse drone-based applications and services become more realistic and are expected to continue growing for personal and professional interest.

Acknowledgements

This work was supported by FCT through the LASIGE Research Unit, ref. UIDB/00408/2020 and ref. UIDP/00408/2020.

References

[1] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, “Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs),” *20th IEEE Int. Symp. A World Wireless, Mob. Multimed. Networks, WoWMoM 2019*, no. C, 2019.

[2] W. Shi, H. Zhou, J. Li, W. Xu, N. Zhang, and X. Shen, “Drone Assisted Vehicular Networks: Architecture, Challenges and Opportunities,” *IEEE Netw.*, vol. 32, no. 3, pp. 130–137, May 2018.

[3] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, “Blind detection: Advanced techniques for WiFi-based drone surveillance,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 938–946, Jan. 2019.

[4] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security services using

blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, Jan. 2019.

[5] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3796–3838, Oct. 2019.

[6] L. Zhang *et al.*, "A Survey on 5G Millimeter Wave Communications for UAV-Assisted Wireless Networks," *IEEE Access*, vol. 7, pp. 117460–117504, Jul. 2019.

[7] A. Fotouhi *et al.*, "Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.

[8] I. Bor-Yaliniz, M. Salem, G. Senerath, and H. Yanikomeroglu, "Is 5G ready for drones: A look into contemporary and prospective wireless networks from a standardization perspective," *IEEE Wirel. Commun.*, vol. 26, no. 1, pp. 18–27, Feb. 2019.

[9] R. R. Guimarães *et al.*, "Intelligent Network Security Monitoring Based on Optimum-Path Forest Clustering," *IEEE Netw.*, vol. 33, no. 2, pp. 126–131, Mar. 2019.

[10] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K. K. R. Choo, "Neural-Blockchain-Based Ultrareliable Caching for Edge-Enabled UAV Networks," *IEEE Trans. Ind. Informatics*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.

[11] W. Shi *et al.*, "Multi-Drone 3-D Trajectory Planning and Scheduling in Drone-Assisted Radio Access Networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8145–8158, Jun. 2019.

[12] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May 2019.

[13] P. Yang, X. Cao, X. Xi, W. Du, Z. Xiao, and D. Wu, "Three-dimensional continuous movement control of drone cells for energy-efficient communication coverage," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6535–6546, Jul. 2019.

[14] K. Lei, Q. Zhang, J. Lou, B. Bai, and K. Xu, "Securing ICN-Based UAV Ad Hoc Networks with Blockchain," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 26–32, Jun. 2019.

[15] X. Wang *et al.*, "Millimeter wave communication: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 1616–1653, Jul. 2018.

Authors short bios

Tao Han (hant@dgut.edu.cn) received the M.E. degree in communication and information system from the South China University of Technology, Guangzhou, China, in 2006, and the Ph.D. degree in communication and information systems from Sun Yat-Sen University, Guangzhou, in 2011. He is currently a Lecturer with the DGUT-CNAM Institute, Dongguan University of Technology, Dongguan, China. He has several years of experience in research, academia, and teaching. His research interests include wearable sensing technology, biomedical signal sensing and processing, body sensor networks, biofeedback, biometric security, Internet of Things, and multimodal medical data fusion.

Igor de L. Ribeiro (firstbrhere@edu.unifor.br) is an undergraduate student in Control and Automation Engineering at the University of Fortaleza (UNIFOR). His research interests include Swarm Technology and Artificial Neural Networks.

Naercio Magaia (ndmagaia@fc.ul.pt) received his Ph.D. in Electrical and Computer Engineering from Instituto Superior Técnico (IST), University of Lisbon (ULisboa). He holds a degree in Electrical Engineering from Eduardo Mondlane University, and an M.Sc. degree in Communication Networks Engineering from IST, ULisboa. He is currently an Invited Assistant Professor at the Faculty of Sciences of ULisboa. His current research interests cover wireless networks, Network Protocols, Network Security, Artificial Intelligence, and Programmable Networks.

João Preto (jpreto@lasige.di.fc.ul.pt) is a final year undergraduate student of Computer Science at the Faculty of Sciences of the University of Lisbon. His research interests are Internet of Vehicles, Fog/Edge Computing and Network Security.

Afonso H. Fontes N. Segundo (afonsof@unifor.br) graduated as a Control and Automation Engineer with an emphasis in Robotics and has a Master of Science degree in Computer Science, in the line of study of artificial intelligence and software development. Today working as an Assistant Professor and Researcher at the University of Fortaleza (UNIFOR), in which, among other subjects, teach the disciplines of Robotics, Autonomous Systems, and Digital Control, areas where most of his research is focused today. He is also a business partner in a solution development company incubated in UNIFOR, where he works as head of development.

Antônio Roberto L. de Macêdo (boblmacedo@unifor.br) is a Ph.D. student at Unifor, Fortaleza. He Graduated in Electronic Engineering in 2004 from the University of Fortaleza / UNIFOR. He received his specialization in Petroleum Engineering in 2014 from UNIFOR and graduated from the College of War in Defense Resource Management in the same year. He received Master in Engineering in 2016 from IFCE. His research interests include medical data analysis using computationally intelligent techniques. He has various publications in reputed journals including European journal of physical and rehabilitation medicine, clinical biomechanics.

Khan Muhammad [S'16, M'18] (khan.muhammad@ieee.org) is an assistant professor at Department of Software, Sejong University, South Korea. His research interests include video summarization, computer vision, big data analytics, IoT, 5G, intelligent transportation, and video surveillance. He has authored over 100 papers in peer-reviewed international journals, such as IEEE COMMAG, NETWORK, TII, TIE, IoJT, TNNLS and TSMC-Systems, and is a reviewer of over 70 SCI/SCIE journals, including IEEE COMMAG, WCOMM, NETWORK, IoTJ, TIP, TII, TCYB, Access and ACM TOMM. He is a member of the ACM.

Victor Hugo C. de Albuquerque [M'17, SM'19] is a full professor and senior researcher at the University of Fortaleza, UNIFOR and Data Science Director at the Superintendency for Research and Public Safety Strategy of Ceará State, Brazil. He has a Ph.D in Mechanical Engineering from the Federal University of Paraíba, an MSc in Teleinformatics Engineering from the Federal University of Ceará and Bachelor in Mechatronics Engineering from the Federal Center of Technological Education of Ceará. He leads the Graduate Program in Applied Informatics and Electronics and Health Research Group (CNPq). He mainly researches IoT, Machine/Deep Learning, Pattern Recognition, and Robotics.